PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN LAS ORGANIZACIONES

ADRIANA OÑATE ARBOLEDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN LAS ORGANIZACIONES

ADRIANA OÑATE ARBOLEDA

Proyecto de Grado – Monografía presentado para optar por el titulo de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Nombre
Edgar Mauricio López Rojas
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Con amor dedico éste trabajo a mi hijo, que con su carisma y comprensión me acompañó en cada etapa vivida, colaborándome de manera indirecta, minimizando mis preocupaciones de madre, también lo dedico a mi mamá que con su apoyo, consagración y paciencia disminuyo mis tareas en el hogar permitiéndome una entrega mas tranquila en el estudio y trabajo.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

pág.

INTRODUCCIÓN 14
1. DEFINICIÓN DEL PROBLEMA 16
1.1 ANTECEDENTES DEL PROBLEMA 16
1.2 FORMULACIÓN DEL PROBLEMA 16
2 JUSTIFICACIÓN 18
3 OBJETIVOS 19
3.1 OBJETIVOS GENERAL 19
3.2 OBJETIVOS ESPECÍFICOS 19
4 MARCO REFERENCIAL 20
4.1 MARCO TEÓRICO 20
4.1.1 Activo de Información 20
4.1.2 Seguridad de la información 20
4.1.3 Norma ISO 27001 22
4.1.4 Ciclo PDCA 23
4.1.5 Análisis de riesgos 25
4.2 MARCO CONCEPTUAL 26
4.2.1 Políticas de seguridad 26
4.2.2 Seguridad de la información: 27
4.2.3 Visión general de la administración de riesgo 28
4.2.4 Magerit 30
4.3 MARCO LEGAL 32
4.3.1 Ley 1266 de 2008: 32
4.3.2 Ley 527 de 1999: 32
4.3.3 Ley 1273 de 2009: 32
4.3.4 Ley 1581 de 2012: 33
4.3.5 Ley 1712 de 2014: 33
5 DESARROLLO DE LOS OBJETIVOS 34
5.1 CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN 34
5.1.1 Inventario de activos 35
5.1.2 Clasificación de activos de información. 37
5.1.3 Clasificación según impacto 39
5.1.4 Criterios de valoración 39

5.2 DEFINICIÓN DE CONTROLES A IMPLEMENTAR SEGÚN LA DECLARACIÓN DE APLICABILIDAD SoA ALINEADA A LA NORMA ISO 27001:2013 40
5.3 Propuesta DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN ALINEADAS CON LA NORMA ISO 27001:2013 49
5.3.1 Políticas de seguridad de la información 49
5.3.2 Gestión de activos de información 52
5.3.3 Control de acceso lógico a la información 54
5.3.4 Áreas Seguras 57
5.3.5 Seguridad en la Operación de la infraestructura de TI 57
5.3.6 Seguridad en las telecomunicaciones 63
5.3.7 Adquisición, desarrollo y mantenimiento de los sistemas de información 65
5.3.8 Seguridad en las relaciones con terceros 68
5.3.9 Seguridad en la continuidad del Negocio de la Organización 69
5.3.10 Cumplimiento de los requisitos legales y contractuales 71
6 CONCLUSIONES 73
7 BIBLIOGRAFÍA 76

LISTA DE FIGURAS

Pág.

Figura 1. ISO 27001:2013 Sistema de Gestión de Seguridad de la Información...22
Figura 2. Comparativo de la norma ISO 27001:2005 vs ISO 27001:2013 23
Figura 3. Fases del ciclo PDCA 24
Figura 4. Fuente Área de Planeación – AS/MSS. 4360- Risk Management 28
Figura 5. Metodología de análisis y gestión de riesgos de los sistemas de información 31
Figura 6. Guía para la gestión y clasificación de activos de información – Mintic..36

LISTA DE TABLAS

Pág.

Tabla 5. Clasificación activos de Información 34
Tabla 7. Clasificación activos de Información 37
Tabla 8. Criterios de Valoración.....39
Tabla 9. Anexo A ISO 27001 40

GLOSARIO

Activo de información: Cualquier componente humano, software, tecnológico, documental o infraestructura, que soportan uno o mas procesos de la organización y en consecuencia debe ser protegido.

Autenticación: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico cuando accede a un sistema de información.

Clasificación de información: Es la decisión para asignar un nivel de sensibilidad a los datos cuando se crea, corrige, almacena o transmite. Debe usarse para crear un conjunto apropiado de niveles de protección.

Código malicioso: El software malicioso incluye todos los programas que codifican deliberadamente para causar un acontecimiento inesperado en el PC de un usuario.

Confidencialidad: Es la información que no está disponible a personas o entidades no autorizadas.

Control: Es toda actividad encaminada a mitigar un riesgo. Incluye políticas Procedimientos, guías, estructuras organizacionales y buenas prácticas.

Disponibilidad: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Incidente de seguridad: Es un evento adverso, confirmado o sospechoso, que haya vulnerado la seguridad de la información o que intente vulnerar, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen.

Inventario de activos de información: Es una lista ordenada y documentada de los activos de información pertenecientes a la organización.

Política de seguridad: Conjunto de reglas, protocolos, normas e Instrucciones documentadas que velan por la seguridad de la información dentro de una organización.

Recursos tecnológicos: Componentes de hardware y software como, servidores, estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red y base de datos entre otros.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Seguridad de la información: Conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información.

Usuarios: Personal de planta, clientes, personal en misión, proveedores, practicantes.

Vulnerabilidades: Debilidades de seguridad inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la empresa, las cuales se constituyen en fuentes de riesgos.

RESUMEN

Dentro del diseño se define un aspecto fundamental en seguridad informática en donde se evalúan las herramientas tecnológicas para asegurar, aplicar, monitorear algunos componentes establecidos en la política de seguridad para evitar ataques a los sistemas de información y que sea de uso obligatorio de los usuarios en las organizaciones.

La política de seguridad se debe sensibilizar con todas las partes interesadas iniciando con la alta dirección quienes avalan para luego socializar con empleados, terceros, ya que se debe estructurar, identificar, detectar, relacionar, proporcionar todas las vulnerabilidades para realizar una evaluación de riesgos y aplicar controles necesarios para reducir el impacto vs la consecuencia dejando los riesgos a un nivel residual bajo.

La política debe ser fácil de comprender, concisa para los usuarios, deben enmarcar las guías y las actividades de una organización, se deben aplicar según las directrices en donde se especifica el estándar y/o norma a utilizar como la ISO 27001:2013 protegiendo la información de cualquier amenaza.

Se debe tener Comprensión y entendimiento de los requerimientos de seguridad y la Identificación de aspectos legales, comerciales y regulatorios relacionados con seguridad de la información.

Palabras claves: Sistema de gestión de seguridad de la información, políticas, Riesgos, Activos de Información, Confidencialidad, Integridad, disponibilidad.

ABSTRACT

The design of information security policies arises from the need to protect information assets and protect them from unauthorized access, preserving the three fundamental principles of information integrity, availability and confidentiality in organizations.

Within the design, a fundamental aspect of computer security is defined, where technological tools are evaluated to ensure, apply, and monitor some components established in the security policy to prevent attacks on information systems and make it mandatory for users to the organizations.
The security policy must be sensitized with all interested parties such as employees, third parties, since it must be structured to identify detect, relate, provide all vulnerabilities to carry out a risk assessment and apply necessary controls to reduce the impact vs. the consequence, leaving the risks at a low residual level.

The policy must be easy to understand, concise and easy to fulfill for all users, they must frame the guidelines and activities of an organization, they must be applied according to the guidelines where the standard and / or norm to be used to protect the information is specified from any threat.
You must have an understanding and understanding of the information security requirements and identification of the legal, commercial and regulatory aspects related to information security

Key words: Information security management system, policies, Risks, Information Assets, Confidentiality, Integrity, availability.

INTRODUCCIÓN

Las tecnologías de la información generan ciertos beneficios, mejorando la prestación de servicios y haciendo más fácil el cumplimiento de su misión y objetivos estratégicos, sin embargo, hace que se enfrenten a riesgos que pueden afectar drásticamente la integridad, confidencialidad y disponibilidad de la información y los recursos de TI que soportan su procesamiento y transmisión.

Para enfrentar este reto y teniendo en cuenta que la información es un activo muy importante para la Organización, es necesario implementar estrategias y controles que garanticen altos niveles de seguridad a la información, por medio de un Sistema de Gestión de Seguridad de la Información alineado a la norma internacional NTC / ISO 27001:2013.

El Sistema de Gestión de Seguridad de la Información basa su funcionamiento en procesos utilizando el modelo PHVA para identificar, implementar, mantener y mejorar los controles necesarios para identificar y gestionar los riesgos inherentes o potenciales de seguridad de la información y ciberseguridad llevándolos a niveles aceptables de riesgo residual.

En las organizaciones se debe hacer énfasis en los siguientes aspectos:

- Comprender y entender de los requerimientos de seguridad de la información y ciberseguridad.
- Identificar los aspectos legales, comerciales y regulatorios relacionados con la seguridad de la información.
- Determinar los activos de información y su clasificación según impacto.

- Valorar y gestionar los riesgos inherentes o potenciales de seguridad de la información y ciberseguridad de los procesos que hacen parte del alcance del SGSI.
- Incluir en el plan de tratamiento de riesgos, los controles definidos en las normas ISO 27001:2013 e ISO 27032:2012

La falta de políticas de seguridad de la información es un problema que confronta las organizaciones con respecto al uso y protección de los activos de información y los riesgos que se encuentran expuestos por situaciones externas e internas.

Las políticas de seguridad indican como operar la seguridad e implementan medidas de protección como: identificación de usuarios, control de acceso físico/lógico, respaldo de información, detección de intrusos y plan de contingencia.

Las políticas tienen complementos de normas, instrucciones, procedimientos, son obligatorias y las directrices son opcionales. También son superiores a las normas, estándares, procedimientos y deben ser acatados.

La propuesta permite que cualquier organización trabaje bajo lineamientos de seguridad y cumplir con requisitos legales a los cuales este obligado la entidad, así mismo es una guía para funcionarios o terceros para que sean responsables sobre la integridad, disponibilidad y confidencialidad de la información.

La idea de este trabajo es colocar en contexto a cualquier persona que está interesada en el tema y aprenda de forma rápida y simple a valorar los datos en cualquier ámbito organizacional y cuente con controles o sistemas de seguridad para mitigar el riesgo de pérdida, robo o fuga de información.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Debido a el desconocimiento de medidas de seguridad, el uso inadecuado de la información, los avances tecnológicos y su impacto en diferentes áreas de nuestro diario vivir, surgen comportamientos inadecuados, que llevan a las organizaciones a conocer, adoptar medidas y buenas prácticas en sus sistemas de información, su infraestructura, sus redes, el recurso humano, que garanticen la sostenibilidad de las actividades del negocio. Mantener la confidencialidad, integridad y disponibilidad de la información es de vital importancia y también surge la necesidad de otro componente que son los profesionales en las áreas de seguridad que deben certificar, monitorear y mantener la seguridad en sus sistemas de información.

La definición de políticas de seguridad de la información cumple un papel importante al interior de las organizaciones para proteger la información y reducir las amenazas que pueden tener los activos de información en las organizaciones aplicando el estándar ISO 27001:2013.

1.2 FORMULACIÓN DEL PROBLEMA

La información es un activo muy valioso y por esta razón se deben proteger de ataques, virus informáticos, denegación de servicios, suplantación de identidad o incidentes de seguridad.

Los mayores incidentes relacionados con los sistemas de gestión de seguridad de la información se deben a pérdida de información, la carencia de sensibilización a los usuarios, falta de recursos económicos, asignación de presupuesto, falta de

especialistas y profesionales, infraestructura obsoleta, dedicados al área de seguridad informática, estos aspectos afectan la seguridad en las organizaciones.

La carencia de políticas de seguridad y el uso inapropiado de las herramientas tecnológicas de los usuarios pueden presentar afectaciones mayores en los sectores empresariales de Colombia.

¿Cómo proponer la implementación de políticas de seguridad de la información para proteger los activos de información en las organizaciones?

2 JUSTIFICACIÓN

La información es el activo más importante de las organizaciones no por su valor económico si no por lo que representa, la información debe administrar las operaciones de negocio y por eso se debe proteger.

Las políticas de seguridad incluyen medidas preventivas realizando una mejora continua, para proteger la información y almacenarla desde que se crea hasta que se destruye, evitando de esta forma la fuga de información, robo o manipulación.

En la actualidad se presentan grandes falencias de seguridad de la información en las diferentes áreas de las organizaciones, por tanto, es preciso revisar las diferentes vulnerabilidades que se presenta en la protección de los datos y los lineamientos para la seguridad. Con el diseño de políticas se dan a conocer controles, guías y buenas prácticas para detectar vulnerabilidades y buscar herramientas que ayuden a mitigar los riesgos. Se requiere de profesionales que apoyen al diseño de las soluciones, realizando seguimiento, auditorias permanentemente.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Plantear políticas de Seguridad de la Información

3.2 OBJETIVOS ESPECÍFICOS

- Clasificar los activos de informaciónsegún el impacto que genera la pérdida de confidencialidad, integridad y disponibilidad.
- mplementar controles según la declaración de aplicabilidad SOA alineada a la norma ISO 27001:2013
- Proponer políticas de seguridad de la información.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Activo de Información

Los activos de información contienen, procesan, almacenan o transmiten información. La información existe de manera impresa, escrita en papel, almacenada electrónicamente y se clasifican en:

- Información lógica, Bases de datos, archivos, documentación de los sistemas, manuales.
- Documentos físicos.
- Software, aplicaciones, sistemas operativos.
- Activos físicos, PC, medios de almacenamiento, cintas, discos, equipos de comunicación.
- Recurso humano
- Servicios de soporte prestados por terceros.[1]

4.1.2 Seguridad de la información

Conjunto de metodologías, recursos, políticas, estrategias, practicas para proteger, la confidencialidad, integridad y la disponibilidad de la información almacenada, ejecutada o procesada en los sistemas informáticos de las organizaciones.

[1] Guía para la gestión y clasificación de activos de información [Sitio web] Bogotá [Consulta: 15 noviembre 2020] Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Uno de los principales objetivos consiste en asegurar los recursos del Sistema de Información de una empresa haciendo uso como lo haya dispuesto la organización, el acceso a la información se debe controlar de la modificación y las personas autorizadas la pueden usar dentro de los límites establecidos.

Los tres pilares fundamentales de la seguridad de la información son:

- Integridad: La propiedad de proteger la precisión y totalidad de los activos.
- Confidencialidad: Propiedad por la cual la información esta disponible solo al personal autorizado.
- Disponibilidad: La propiedad que puede acceder y ser utilizada al personal autorizado.[2]

El sistema de Gestión de Seguridad de la información comprende un conjunto de estándares destinada a guiar a cualquier tipo de organización a implementar y operar un SGSI y esta constituida por las siguientes series:

[2]Protección de la información INCIBE [Sitio web] Bogotá [Consulta: 15 noviembre 2020] disponible en https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

En la figura 1 se describe la serie 27000

Figura 1. ISO 27001:2013 Sistema de Gestión de Seguridad de la Información

Fuente: Serie 27000 [Sitio web] ISO 27000.ES [Consultado 15 de marzo 2020] Disponible en https://www.iso27000.es/iso27000.html.

4.1.3 Norma ISO 27001

El Estándar internacional emitido por la ISO que describe como gestionar la seguridad en las organizaciones. La versión mas reciente es de 2013 la primera versión es publicada en el año 2005 basada en las normas británicas BS 7799-2. Esta norma permite el aseguramiento, la confidencialidad, integridad y disponibilidad de los datos, así como los datos que se procesan. Permite a las organizaciones evaluar los riesgos y aplicar controles necesarios para reducirlos.

La ISO 27001 se puede implementar en cualquier tipo de organización, privada, publica, pequeña, grande, permitiendo la certificación del estándar según el cumplimiento.

ISO 27001 está dividida en 11 secciones, adicional el anexo A; En las secciones de la 0 a 3 no son obligatorias para la implementación, las secciones de la 4 a 10 si son obligatorias. Los controles se implementan si corresponden a la declaración de aplicabilidad.[3]

En la figura 2 se observa la estructura del Anexo ISO 27001:2005 Vs ISO 27001:2012

Figura 2. Comparativo de la norma ISO 27001:2005 vs ISO 27001:2013

Fuente: Giraldo González Eduin. Comparativo de la norma ISO 27001:2005 vs ISO 27001:2013 [Sitio web] [Consultado:15 de marzo 2020] https://prezi.com/rf6wx2d4xfgf/comparativo-de-la-norma-iso-270012013-vs-iso-270012005/

4.1.4 Ciclo PDCA

Todos los sistemas de gestión adoptan el ciclo como metodología aplicable a todos los procesos. Conocida por sus siglas en Ingles PDCA Plan -Do- Check -Act. Es un

[3] Norma ISO 27001 [Sitio web] Bogotá [Consulta: 15 noviembre 2020] Disponible https://normaiso27001.es/

concepto que se desarrolló hace 60 años por Edwards Deming Consultor de gestión de Calidad basa su funcionamiento en 4 fases[4]:

- Fase Plan: Antes de comenzar a implementar de debe conocer lo que se requiere y que se desea lograr (objetivos).
- Fase Do (Hacer): Una vez se tengan los objetivos, se puede iniciar la implementación según el enfoque que tenga cada estándar.
- Fase Verificación: Asegura que se logró lo planeado, se debe monitorear y medir si se logró sus objetivos.
- Fase Actuar: Cuando se identifica que hay vacíos en lo planeado.

En la figura 3 metodología PDCA y sus fases.

Figura 3. Fases del ciclo PDCA

Fuente: BETANCOURT, Diego. *Ciclo de Deming (PDCA): Qué es y cómo logra la mejora continua*. [En línea]. 02 de agosto de 2018. [Citado 24 de marzo de 2021]. Disponible en: www.ingenioempresa.com/ciclo-pdca

[4] ISO/IEC 27001:2013 - Ciclo de mejora continua o Deming [Sitio web] Bogotá [Consulta: 15 noviembre 2020] disponible en http://seguridadinfoperu.blogspot.com/2017/05/isoiec-270012013-ciclo-de-mejora.html

4.1.5 Análisis de riesgos

Existen técnicas de aseguramiento para los activos de información ya que es un aspecto muy importante, la seguridad física se establece de acuerdo con los equipos que estén destinados a almacenar información de las organizaciones.

La seguridad lógica soporta la información, aplicando instrucciones que protegen y restringen el acceso a todos los datos al personal no autorizado.

Características principales:

- Restricción de acceso, Uso de archivos y/o programas para los usuarios
- Los usuarios deben realizar sus labores sin modificar programas ni archivos sin autorización.
- Certificar que la información en tránsito de salida sea la misma que se reciba el destinatario.
- En caso de emergencia o desastre se debe garantizar que existan los sistemas necesarios para accionarlos en la organización.
- Los usuarios son únicos e intransferibles, no se debe compartir las contraseñas.
- Actualizar periódicamente las contraseñas de ingreso a los sistemas de información.

Para ejecutar las políticas de seguridad se debe asegurar el mínimo privilegio de acceso a los datos y sistemas con que cuente la organización, realizar un monitoreo para controlar los mecanismos de identificación y asegurar que utilizan los privilegios asignados para sus labores[5].

[5] Análisis de riesgo en 6 pasos [Sitio web] Bogotá [Consulta: 15 noviembre 2020]disponible en https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

4.2 MARCO CONCEPTUAL

4.2.1 Políticas de seguridad

Es un documento que define el alcance de la seguridad que necesitan las organizaciones, define los activos que necesitan protección y las actividades por las cuales las soluciones de seguridad deberían proveer la protección requerida.

Es una visión generalizada de las necesidades de seguridad de una organización, que define claramente porque la seguridad es importante y cuales activos son valiosos para la empresa[6].

La política de seguridad se utiliza para asignar responsabilidades, bosquejar el proceso de obligatoriedad y definir los niveles aceptables de riesgo.

Tipos de políticas de seguridad:

- Regulatorias: Son políticas de seguridad requeridas cuando existen normas de la industria o estándares legales aplicables a la organización. Definen la normatividad que debe ser cumplida y los procedimientos que se deben seguir para lograr este cumplimiento.
- Sugeridas: Son políticas de seguridad que definen comportamientos y actividades aceptables en la organización y especifican las consecuencias por violaciones.
- Informativas: Son políticas de seguridad diseñadas para proveer información o conocimiento respecto a temas específicos, tales como los objetivos organizacionales, la misión empresarial o la manera como interactúa la organización con socios y clientes.

[6] Política de seguridad de la información [Sitio web] Bogotá [Consulta: 15 noviembre 2020] disponible en https://normaiso27001.es/a5-politicas-de-seguridad-de-la-informacion/

4.2.2 Seguridad de la información:

Es el conjunto de, estrategias, políticas, metodologías, soluciones informáticas, recursos, para asegurar, proteger y preservar los tres pilares fundamentales de la seguridad de la información que se almacene, en los sistemas de información.

Activo de información: Son componentes (tecnológico, humano, infraestructura software, documental) que soportan los procesos de la compañía y deben ser protegidos.

Análisis de riesgos de seguridad de la información: Permite establecer el riesgo asociado con la amenaza. Califica la probabilidad de ocurrencia y el impacto de consecuencias utilizando un método cualitativo.

Confidencialidad: Propiedad por la cual la información está disponible solo al personal autorizado[7].

Control: Actividad enfocada a reducir un riesgo de carácter administrativo, físico, tecnológico o legal[8].

Disponibilidad: La propiedad que puede acceder y ser utilizada al personal autorizado[9].

Incidente de Seguridad: Intento de acceso, divulgación, destrucción o modificación no autorizado.

[7]Confidencialidad [Sitio web] Bogotá [Consulta: 15 noviembre 2020] en https://es.wikipedia.org/wiki/Confidencialidad
[8] Controles de seguridad y privacidad de la información
[9]Disponibilidad [Sitio web] Bogotá [Consulta: 15 noviembre 2020] disponible en https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

Integridad: La propiedad de proteger la precisión y totalidad de los activos[10].

Riesgo: Grado de exposición de un activo el cual permite la materialización de una amenaza ocasionando daños a la compañía.

SGSI: Sistema de Gestión de Seguridad de la Información.

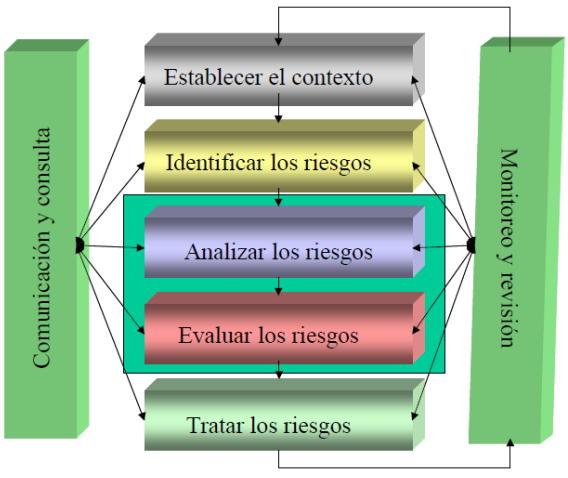
Vulnerabilidad: Son debilidades que afectan activos de información y pueden ser explotadas por autores externos que constituyen fuentes de riesgo.

4.2.3 Visión general de la administración de riesgo

Es un proceso iterativo de mejoramiento continuo, que se lleva mejor a cabo con la participación de un grupo multidisciplinario.

En la figura 4 descripción de la versión AS / NZS 4360.

Figura 4. Fuente Área de Planeación – AS/MSS. 4360- Risk Management



[10]Integridad [Sitio web] Bogotá [Consulta: 15 noviembre 2020] disponible en https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

Fuente: Gestión de riesgos empresariales [Sitio web] [Consultado 18 de febrero 2020] Disponible en https://www.lexology.com/library/detail.aspx?g=8872e62a-689f-4eab-bc6f-f8261ef64bb9

Los elementos principales del proceso de administración del riesgo son los siguientes:

Establecer el contexto. Establecer el contexto estratégico, organizacional y de administración y establecer los criterios contra los cuales se evaluarán los riesgos y definir la estructura del análisis.

Identificación de riesgos. Identificar qué, por qué y cómo las cosas pueden suceder como la base para mayores análisis.

Análisis de riesgos. Se establecen los controles y los riesgos analizados en términos de consecuencia*probabilidad considerando el rango de consecuencias potenciales y como posiblemente esas consecuencias pueden materializar. La combinación de la consecuencia y la probabilidad producen un nivel de riesgo estimado.

Evaluación de riesgos. Comparar los niveles de riesgo estimados contra el criterio preestablecido. Esto permite priorizar los riesgos, así como identificar las prioridades de la administración. Si los niveles de riesgo establecido son bajos, entonces los riesgos podrían caer en una categoría aceptable y podría no necesitarse un tratamiento.

Tratamiento de riesgos. Aceptar y monitorear los riesgos de bajos. Para los riesgos críticos y altos se implementa plan de manejo específico incluyendo consideraciones de fundamento.

Monitorear y revisar. Monitorear y revisar el desempeño del sistema de administración y los cambios que podrían afectarlo.

Comunicación y consulta. Apropiada con accionistas internos y externos, no solo en cada estado del proceso de administración del riesgo sino en cada estado del proceso de administración del riesgo sino en lo concerniente a la totalidad del proceso.

La administración del riesgo se puede aplicar en diferentes contextos de las organizaciones tanto a nivel estratégico como a nivel operativo, también se puede aplicar a proyectos específicos para asistir decisiones específicas o para manejar áreas de riesgo reconocido[11].

4.2.4 Magerit

Es una metodología enfocada al análisis y gestión de riesgo creada por el concejo superior de administración electrónica, como respuesta a la percepción de la sociedad, dependen de la tecnología de información para el cumplimiento de su misión.

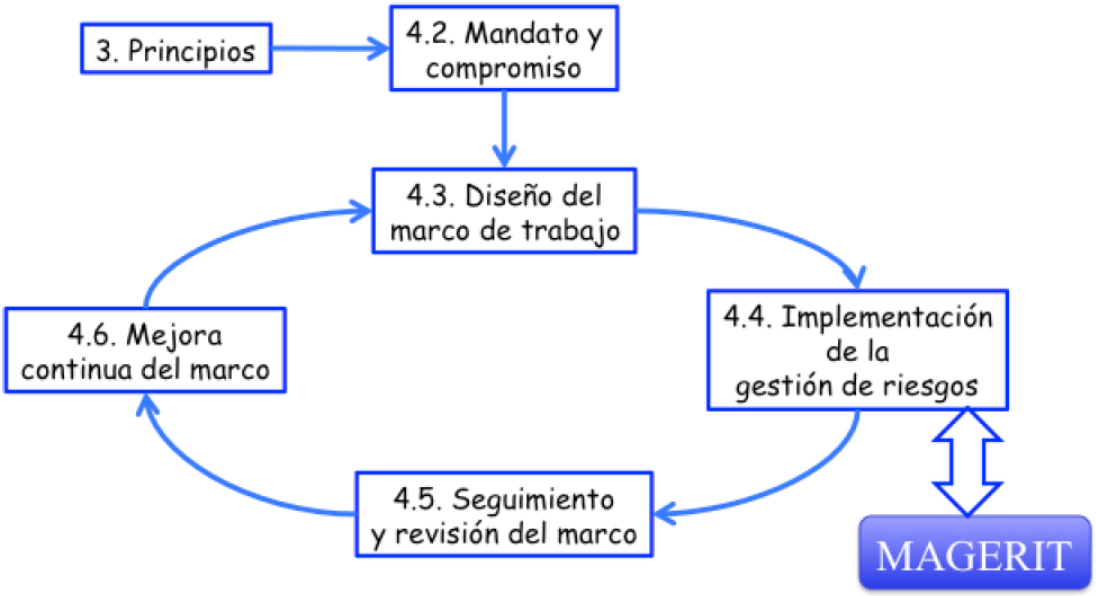
Magerit está directamente relacionada con el uso de la tecnología y genera uno beneficios a la comunidad; pero también hay riesgos que se deben reducir con medidas de seguridad que den confianza.

La metodología contempla actividades enfocadas a los activos que una organización tiene para el tratamiento de la información.

[11] Análisis de riesgos en 6 pasos [Sitio web] Bogotá [Consulta: 15 noviembre 2020] disponible en https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

En la figura 5 se observa el proceso de Gestión de Riesgos, basado en la ISO 31000.

Figura 5. Metodología de análisis y gestión de riesgos de los sistemas de información



Fuente: Magerit V3 Metodología de análisis y gestión del riesgo de los sistemas de información [Sitio web] [Consultado: 5 abril 2020] disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.X6nBV6Kfga_

La metodología cuenta con los siguientes objetivos directos:

- Concienciar a los responsables de las organizaciones sobre la existencia de los riesgos y la necesidad de gestionarlos.
- Ofrece un método sistemático para analizar los riesgos relacionados con los sistemas de información y comunicaciones.
- Planifica el tratamiento oportuno para mantener los riesgos bajo control.

Objetivos indirectos:

- Prepara a las organizaciones para procesos de evaluación, auditoria, certificación, según corresponda.
- Uniformidad en los informes de hallazgos y conclusiones de las actividades de análisis y gestión de riesgos[12].

4.3 MARCO LEGAL

4.3.1 Ley 1266 de 2008:

Disposiciones generales habeas data, manejo de información contenida en bases de datos personales, información financiera, crediticia y la proveniente de terceros países[13].

4.3.2 Ley 527 de 1999:

Reglamenta el acceso y uso de mensajes de datos, comercio electrónico, firmas digitales.

4.3.3 Ley 1273 de 2009:

Modificación de código penal denominado “protección de la información y de datos y se preservan los sistemas de información y comunicaciones[14].

[12] Magerit V3 Metodología de análisis y gestión del riesgo de los sistemas de información [Sitio web] Bogotá [Consulta: 15 noviembre 2020] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.X6nBV6Kfga_

[13] Ley estatutaria 1266 de 2008 [Sitio web] Bogotá [Consulta: 15 noviembre 2020] disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

[14]Legislación informática de Colombia [Sitio web] Bogotá [Consulta: 15 noviembre 2020] disponible en

4.3.4 Ley 1581 de 2012:

Protección de datos personales.

4.3.5 Ley 1712 de 2014:

Ley de transparencia y derecho de acceso a la información publica

http://www.informaticajuridica.com/legislacion/colombia/#:~:text=Ley%201273%20de%205%20de,y%20las%20comunicaciones%2C%20entre%20otras

5 DESARROLLO DE LOS OBJETIVOS

5.1 CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

El objetivo principal en la clasificación de activos es asegurar los niveles de protección adecuados y de acuerdo con su valor y otras características se determina el manejo que requiere.

La clasificación de la información tiene características particulares y contempla la cultura y funcionamiento interno de las organizaciones para cumplir con los requerimientos estipulados en la norma ISO 27001:2013.

En la clasificación de activos de información se valoran los tres pilares fundamentales de la seguridad de la información que son: confidencialidad, integridad y disponibilidad.

Tabla 6. Clasificación activos de Información

Impacto	Confidencialidad	Integridad	Disponibilidad
Muy Alto	La pérdida de confidencialidad es extremadamente perjudicial para la organización.	La pérdida de integridad es extremadamente perjudicial para la organización.	La pérdida de disponibilidad es extremadamente perjudicial para la organización.
Alto	La pérdida de confidencialidad es	La pérdida de integridad es	La pérdida de disponibilidad es

	altamente perjudicial para la organización.	altamente perjudicial para la organización.	altamente perjudicial para la organización .
Medio	La pérdida de confidencialidad es medianamente perjudicial para la organización.	La pérdida de integridad es medianamente perjudicial para la organización.	La pérdida de disponibilidad es medianamente perjudicial para la organización.
Bajo	La pérdida de confidencialidad es poco perjudicial para la organización.	La pérdida de integridad es poco perjudicial para la organización.	La pérdida de disponibilidad es poco perjudicial para la organización.
Muy Bajo	La pérdida de confidencialidad no es perjudicial para la organización o no aplica para el activo.	La pérdida de integridad no es perjudicial para la organización o no aplica para el activo.	La pérdida de disponibilidad no es perjudicial para la organización o no aplica para el activo.

Fuente: Elaboración Propia. Criterios de clasificación alineados con los tipos de información declarados en la ley 1712 del 2014

5.1.1 Inventario de activos

La identificación de inventario de activos consiste en clasificar el tipo de información y validar a los que se le debe brindar mayor protección, identificando sus características y roles al interior de un proceso[15].

En la figura 6 se describen las actividades para ejecutar el inventario de activos.

Figura 6. Guía para la gestión y clasificación de activos de información – Mintic

Fuente: Procedimiento para inventario de activos https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

[15] Guía para la gestión y clasificación de activos de información https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

5.1.2 Clasificación de activos de información.

Los activos de información se clasifican según su sensibilidad, criticidad y según las funciones que cumpla en los procesos de las organizaciones. A continuación, la descripción de categorías.

Tabla 7. Clasificación activos de Información

Grupo de Activos	Descripción del grupo de Activos
Información	• Estructurada, almacenada en motores de base de datos. • No Estructurada (Excel, PDF, Docs., Txt. • Información en medio físico.
Software	• Aplicativos desarrollados in-house o adquiridos a terceros. • Código fuente de aplicativos desarrollados in-house. • Sistemas Operativos de estaciones de trabajo y servidores que requieren licencia de uso.
Locaciones/Sitio	• Centros de computo • Datacenter • Oficinas de IT • Diferentes sedes
Servidores	• Servidores de red. • Almacenamiento

	• Aplicativos • Bases de Datos
PC Estaciones de trabajo	• Portátiles • Equipos móviles • Estaciones fijas de trabajo
Red	• Switch • Router • Canales de comunicación • Firewall
Personas	• Funcionarios • Proveedores • Clientes • Socios de negocio.
Infraestructura	• Impresoras • Scanner • UPS • Planta eléctrica
Imagen Reputacional	Imagen reputacional de la organización o de sus funcionarios.

Fuente Elaboración propia

5.1.3 Clasificación según impacto

Información pública: Es la información administrada por las organizaciones y esta a disposición del público en general, su divulgación no requiere de autorización.
Información privada: Es de uso interno en las organizaciones, puede ser compartida con entes externos para el desarrollo de sus negocios. La divulgación de información privada no autorizada puede causar daño moderado.
Información Confidencial: Es información que solo debe conocer exclusivamente las personas autorizadas. La información debe estar restringida, debe usarse con permisos de menor privilegio y la divulgación requiere de permisos y de acuerdos de confidencialidad.

5.1.4 Criterios de valoración

Es la descripción del riesgo de acuerdo con el nivel de seguridad, teniendo en cuenta la valoración cualitativa según la metodología de Magerit.

Se deben promediar los valores numéricos del impacto de la Confidencialidad, la Integridad y la Disponibilidad y con base en el resultado, colocar el valor cualitativo según la siguiente tabla.

Tabla 8. Criterios de Valoración

Nivel de Seguridad	Valor				
	Muy Alto	Alto	Medio	Bajo	Muy Bajo
Confidencialidad	90-100%	61-89%	40-60%	20-39%	0-19%
Integridad					
Disponibilidad					

Fuente Elaboración Propia

5.2 DEFINICIÓN DE CONTROLES A IMPLEMENTAR SEGÚN LA DECLARACIÓN DE APLICABILIDAD SOA ALINEADA A LA NORMA ISO 27001:2013

Se definen controles, para mitigar el impacto cuando el riesgo se materialice en los activos de información relacionados.

Este documento establece e informa a las partes interesadas los controles de la norma ISO 27001:2013 que son relevantes para el Sistema de Gestión de Seguridad de la Información y Ciberseguridad de la Organización.

RL: Requerimiento legal o regulatorio; RN: Requerimiento del Negocio; RC: Requerimiento contractual; AR: Análisis de riesgo.

Tabla 9. Anexo A ISO 27001

DOMINO	CONTROL	DESCRIPCIÓN	SELECCIÓN DE CONTROLES			
			RL	RN	RC	AR
A.5		Políticas de seguridad de la información				
A.5.1.1	Políticas para la seguridad de la información	Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.				

A.5.1.2	Revisión de las políticas para seguridad de la información	Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
A.6	Organización de la seguridad de la información	
A.6.1.1	Seguridad de la información Roles y Responsabilidades	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información
A.7	Seguridad de los recursos humanos	
A.7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.2.1	Responsabilidades de la dirección	Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de

		acuerdo con las políticas y procedimientos establecidos por la organización
A.8		Gestión de activos
A.8.1.1	Inventario de activos	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos
A.8.2.1	Clasificación de la información	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada
A.8.2.3	Manejo de activos	Control: Se debe desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización
A.9		Control de acceso
A.9.1.1	Política de control de acceso	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Política sobre el	Control: Solo se debería permitir acceso de los usuarios a la red y a

	uso de los servicios de red	los servicios de red para los que hayan sido autorizados específicamente
A.9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado
A.9.4.1	Restricción de acceso Información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso
A.9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro
A.9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
A.11	Seguridad física y del entorno	

A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones
A.11.1.4	Protección contra amenazas externas y ambientales	Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.2.2	Servicios de suministro	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.4	Mantenimiento de equipos	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas
A.12		Seguridad de las operaciones
A.12.2.1	Controles contra códigos maliciosos	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos

A.12.3.1	Respaldo de información	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada
A.12.4.1	Registro de eventos	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
A.12.5.1	Instalación de software en sistemas operativos	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos
A.12.6.2	Restriccion es sobre la instalación de software	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.13	Seguridad de las comunicaciones	
A.13.1.1	Controles de redes	Control: Las redes se deberían gestionar y controlar para proteger

		la información en sistemas y aplicaciones.
A.13.2.3	Mensajería electrónica	Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.
A.15	Relación con los proveedores	
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.16	Gestión de incidentes de seguridad de la información	
A.16.1.3	Reporte de debilidades de seguridad	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier

	de la información	debilidad de seguridad de la información observada o sospechada en los sistemas o servicios
A.16.1.7	Recolección de evidencia	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia
A.17	Aspectos de seguridad de la información de la gestión de continuidad de negocio	
A.17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa
A.18	Cumplimiento	
A.18.1.3	Protección de registros	Control: Los registros se deberían proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.

A.18.1.4	Privacidad y protección de datos personales	Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad
A.18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Fuente Elaboración propia

5.3 PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN ALINEADAS CON LA NORMA ISO 27001:2013

5.3.1 Políticas de seguridad de la información.

5.3.1.1 Organización Interna

a. La Alta Dirección define en plan estratégico lo relacionado con la seguridad de la información y delega las responsabilidades de gestión del sistema al comité de seguridad de la información y ciberseguridad.

5.3.1.2 Responsabilidades de la alta dirección

La dirección tiene la responsabilidad de apoyar y conseguir los recursos financieros, logísticos, operacionales y humanos necesarios para desarrollar adecuadamente los proyectos relacionados con la seguridad de la información y ciberseguridad. Adicionalmente, es responsable de:

a. Garantizar los recursos necesarios para el desarrollo del Sistema de Gestión de Seguridad de la Información.
b. Aprobar las directrices de seguridad de la información y ciberseguridad definidas por el comité.
c. Direccionar la estrategia del SGSI y delegar las de gestión del SGSI al comité de seguridad de la información de Organización

5.3.1.3 Comité de seguridad de la información

Responsabilidades del Comité de Seguridad:

a. Revisar y aprobar las políticas de seguridad de la información de La Organización.
b. Liderar los proyectos de seguridad de la información
c. Hacer seguimiento a la gestión de riesgos de seguridad de la información y ciberseguridad.
d. Identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales.
e. Asegurar que todo el personal tiene conciencia de la importancia de la seguridad de la información y el cumplimiento de sus responsabilidades para con el SGSI.
f. Coordinar las revisiones por partes externas del SGSI cuando sea necesario.
g. Evaluar, revisar, aprobar y coordinar la implementación de los controles de seguridad de la información y ciberseguridad.
h. Velar por las actualizaciones independientes a las políticas de seguridad de la información y ciberseguridad, y la efectividad y eficiencia de los controles implementados.
i. Realizar reportes periódicos a la Alta Dirección de La Organización, indicando el nivel de seguridad obtenido.
j. Asegurar la ejecución de actividades de concientización y capacitación a todos los funcionarios que enfatice la importancia del cumplimiento de las políticas seguridad de la información y ciberseguridad y su contribución al logro de los objetivos del negocio.
k. El Comité de Seguridad de la información se reunirá trimestralmente o cuando un incidente de seguridad requiera atención por parte del comité.

5.3.1.4 Oficial de seguridad de la información

Este rol tendrá las siguientes responsabilidades:

a. Documentar las políticas y normas de seguridad de la información y ciberseguridad.
b. Apoyar la identificación, evaluación y control de los riesgos de seguridad de la información y ciberseguridad de los diferentes procesos.
c. Apoyar a los líderes del proceso en la definición, diseño, implementación y monitoreo de los controles para mitigar los riesgos asociados a la seguridad de la información y ciberseguridad
d. Verificar que los planes de tratamiento y controles definidos para mitigar los riesgos de seguridad de la información y ciberseguridad se ejecutan efectiva y eficientemente.
e. Desarrollar actividades de capacitación y concienciación en temas relacionados con la seguridad de los activos de información.
f. Coordinar el desarrollo de auditorías internas al SGSI.
g. Actualizar periódicamente el manual del SGSI y las normas de seguridad de la información y ciberseguridad
h. Participar en grupos y foros de discusión en temas relacionados con la seguridad de la información y ciberseguridad.

5.3.1.5 Jefes de procesos

Los líderes o Líder de procesos de La Organización tienen las siguientes responsabilidades:

a. Verificar el cumplimiento de las políticas, normas, guías y procedimientos de seguridad de la información y ciberseguridad al interior de su proceso.
b. Participación en la identificación de los riesgos y planes de tratamiento
c. Implementar y/o coordinar que los custodios de información implementen los controles definidos para proteger la información confidencial.
d. Identificar y clasificar la información crítica y sensible del proceso.

5.3.1.6 Responsabilidad de los usuarios

a. Todos los usuarios internos o externos que tengan alguna interacción con el uso de activos de información de La Organización deben dar cumplimiento sin ninguna restricción a las políticas y normas de seguridad de la información y ciberseguridad establecidas.
b. Realizar sesiones de sensibilización, capacitación acerca de temas de seguridad de la información y ciberseguridad.

5.3.2 Gestión de activos de información

5.3.2.1 Compromiso Sobre los Activos

5.3.2.1.1 Propiedad o responsabilidad de los activos

a. La Alta Dirección de La Organización establece que los Líderes de procesos son responsables de los activos de información de su proceso.

5.3.2.1.2 Inventario de Activos de Información

a. Los responsables de los activos de información de cada proceso de La Organización deben realizar un inventario de los activos de información (sin importar el medio en cual se encuentren, físico o lógico) a su cargo
b. Los datos mínimos que debe contener el inventario de los activos de información (físicos y magnéticos) son:

    - Nombre Activo de información

- Ubicación física o lógica del activo
- Responsable
- Custodio
- Nivel de clasificación de acuerdo con su confidencialidad.

c. Actualizar el inventario de activos cuando ocurra uno o varios de los siguientes casos:

- Cambios en el ambiente de negocios o estrategia empresarial (ingreso de nuevos clientes).
- Nuevas obligaciones legales, contractuales o reglamentarias relacionadas con la información sensible o confidencial.
- Pasado un año después de la última actualización del inventario.

5.3.2.1.3 Clasificación, Etiquetado y Tratamiento de la Información

a. El líder de procesos es responsable de los activos de información en medio físico y/o magnético, por lo tanto, realizan el inventario y clasificación de los mismos de acuerdo a su valor, requerimientos legales vigentes.
b. Los niveles de confidencialidad en que se deben clasificar los activos de información son:

- Información de uso público o informativo (pública). Su divulgación no requiere de autorización especial dentro o fuera de La Organización y su función es de comunicación al personal en general.
- Información de uso interno o privada (privada). Su divulgación no autorizada, principalmente fuera de La Organización es inadecuada o inconveniente,

debe ser de conocimiento únicamente por parte de los funcionarios de La Organización, clientes o consultores externos debidamente autorizados.

- Información de uso confidencial (confidencial). Sustenta estrategias del negocio, información financiera, informes de gestión para la junta directiva, registros para toma de decisiones a nivel de gerencias, información de clientes, proveedores y competencia, información que contenga datos de personas naturales y cualquier otra que pueda comprometer la seguridad de la empresa, de las personas o sus clientes. Su divulgación no está autorizada, incluso dentro de La Organización, por el impacto que puede causar a la misma.

c. La información de los clientes es clasificada como confidencial en toda La Organización y su manejo debe estar limitado a actividades propias del negocio, no debe ser divulgada a personas no autorizadas.
d. La información clasificada como confidencial que es enviada a terceros debe ser transmitida utilizando mecanismos que garanticen un nivel adecuado de confidencialidad e integridad.
e. El acceso a la información confidencial almacenada en las bases de datos y archivos digitales o físicos debe ser estrictamente controlado y debe otorgarse por parte de los Líderes de proceso de acuerdo a condiciones exclusivas del negocio.

5.3.3 Control de acceso lógico a la información

a. El acceso lógico a todos los sistemas de información de La Organización es controlado mediante un sistema de autenticación y autorización con el fin de prevenir el acceso no autorizado a la información confidencial de La Organización, Clientes y demás partes interesadas.

b. Los privilegios de acceso de los usuarios a los diferentes sistemas de información deben ser autorizados por los Líderes de proceso y deben limitarse al mínimo requerido para cumplir con las responsabilidades propias de su cargo.
c. Garantizar la segregación de funciones en las actividades de autorización, asignación, creación y administración de credenciales en los diferentes sistemas de información.

5.3.3.1 Gestión de acceso de usuarios

a. Establecer el procedimiento formal y documentado para la creación, modificación y eliminación de usuarios en los diferentes sistemas de información. Estos procedimientos incluyen:

    i. La autorización por parte de Líderes de proceso para obtener acceso a los diferentes sistemas de información.
    ii. Verificación que el acceso concedido es el solicitado, el autorizado y el apropiado de acuerdo con el objetivo del negocio, la política de menor privilegio y la autorización del líder de la información.
    iii. Documento de aceptación por parte del usuario solicitante en donde se registra que recibió a satisfacción el usuario creado y que está bajo su responsabilidad a partir de la fecha de recibo.

5.3.3.2 Gestión de contraseñas

a. Las contraseñas de todos los sistemas de información de La Organización cumplen con las siguientes características:

    - Longitud mínima de 8 caracteres
    - Ser alfanumérica
    - Debe contener mayúsculas y minúsculas

b. La contraseña debe expirar periódicamente, se recomienda cada 60 días y debe ser cambiada de manera obligatoria por los usuarios.
c. Los usuarios cambian la contraseña en el primer inicio de sesión.
d. Los sistemas de información no permiten el uso de las últimas cinco contraseñas
e. El acceso a los sistemas de información es bloqueado después de cinco (5) intentos fallidos de ingreso.

5.3.3.3 Responsabilidades de los usuarios

a. Los funcionarios, clientes, proveedores y/o consultores externos que tienen acceso a los sistemas de información de La Organización deben comprometerse a:

- Mantener la confidencialidad del usuario y la contraseña
- Evitar la escritura de las contraseñas en papeles
- Cambiar la contraseña si tiene algún indicio de su vulnerabilidad
- No utilizar contraseñas que estén asociadas con temas de la Organización, números de cedula, direcciones, fechas de cumpleaños, películas, palabras que se encuentren en diccionarios.
- Cambiar periódicamente las contraseñas
- Cambiar las contraseñas la primera vez que inicia sesión.

No incluir las contraseñas en ningún procedimiento automático de conexión, scripts, Shell, mecanismos de recordar contraseñas de navegadores

5.3.4 Áreas Seguras

a. Las áreas seguras necesitan autorización para el ingreso de personas ajenas al área, por la naturaleza de la información confidencial que se maneja o los procesos que allí se realizan.
b. Las áreas seguras deben estar delimitadas físicamente y el acceso físico debe ser controlado.

5.3.4.1 Controles físicos de entrada

a. El ingreso de personal ajeno a las áreas seguras debe ser autorizado por el jefe de área correspondiente.
b. Los visitantes a las áreas seguras deben portar un carnet que los identifique como visitantes.
c. Para todos los visitantes a las áreas seguras, se registrará la fecha y hora de ingreso, funcionario a quien visita y fecha y hora de la salida. El registro de esta información se puede hacer electrónico o en bitácoras manuales

5.3.5 Seguridad en la Operación de la infraestructura de TI

5.3.5.1 Responsabilidades y procedimientos de operación

5.3.5.1.1 Documentación de procedimientos de operación

a. La Dirección de Tecnología debe documentar los procedimientos de operación de la infraestructura tecnológica.
b. Entre otros, los procedimientos que se deben documentar son:

- Inicio y apagado de los equipos de misión crítica
- Backup y restauración de datos
- Control de cambios de hardware y software
- Gestión de incidentes
- Gestión de usuarios, roles y perfiles de seguridad
- Mantenimiento de equipos
- Gestión de registros de auditoría

5.3.5.1.2 Gestión de cambios

a. La Dirección de Tecnología de la organización debe establecer un procedimiento formal y documentado para controlar todos los cambios de hardware y/o software de la infraestructura de TI.
b. Los procedimientos de control de cambios de la infraestructura deben asegurar que:

- Los cambios significativos se identifican y se documentan.
- Los planes del cambio se establecen y se prueban.
- Los impactos potenciales de los cambios se identifican y se analizan, incluyendo los impactos a nivel de confidencialidad, integridad o disponibilidad de la información
- Se obtiene la aprobación formal para los cambios por parte de los dueños de la información afectada por el cambio.
- Los detalles del cambio se comunican a todas las áreas involucradas
- Se documentan las actividades de contingencia para abortar y recuperarse de cambios fallidos.
- Todos los cambios son probados en ambientes controlados por los dueños de la información antes de subir a los ambientes de producción.

c. Los cambios que se realicen sobre los recursos de TI de misión crítica deben ser registrados en una bitácora de cambios.
d. Antes de realizar un cambio de hardware y/o software en los recursos de TI de misión crítica, se debe hacer una copia de respaldo de la información.
e. El procedimiento de control de cambios debe contemplar cambios de emergencia.

5.3.5.1.3 Gestión de capacidades

a. La Dirección de Tecnología debe monitorear todos los recursos de TI con el fin de identificar el nivel de desempeño ofrecido y las necesidades de crecimiento requeridas para satisfacer los requerimientos de la organización.

5.3.5.1.4 Separación de entornos de desarrollo, pruebas y producción

a. La Dirección de Tecnología de la organización debe asegurar que los ambientes de desarrollo de software, pruebas y producción se encuentran en ambientes lógicamente separados y con controles de acceso independientes.
b. La Dirección de Tecnología debe establecer un procedimiento formal y documentado para la transferencia de software entre los ambientes de desarrollo, pruebas y producción.
c. El ambiente de pruebas o calidad debe emular el ambiente de producción tanto como sea posible.
d. La información confidencial que sea necesario trasladar a los ambientes de desarrollo debe ser enmascarada antes de pasarla a desarrollo

5.3.5.1.5 Protección contra código malicioso

a. La Dirección de Tecnología debe garantizar que todos los computadores conectados en la red de la Organización tienen instalado el software antivirus de acuerdo con el estándar vigente.
b. Se deben implantar los mecanismos de actualización permanente y en línea del software antivirus instalado en los computadores conectados en la red. De igual forma, se debe garantizar un mecanismo semiautomático o manual que permita la actualización del antivirus instalado en computadores que no se conectan de manera permanente a la red.
c. Periódicamente se debe monitorear la consola de administración del software antivirus, con el fin de identificar los computadores que no tienen la última versión instalada. De ser necesario, se aplicará un procedimiento manual de actualización por parte del área de informática.
d. El software antivirus debe ser configurado para el escaneo en línea de todas las unidades de almacenamiento.
e. Todo CD, memoria USB, o disco externo que sea conectado en un computador de la organización independientemente de su procedencia, debe ser escaneado con el software antivirus antes de ser utilizado.
f. Los usuarios deben reportar de inmediato al área de soporte cualquier comportamiento anormal del computador o indicio de la presencia de virus, con el fin de prevenir la propagación de este.

5.3.5.1.6 Copias de seguridad

a. La información de los diferentes procesos debe ser almacenada exclusivamente en las unidades de almacenamiento suministradas por la Dirección de Tecnología. No se puede almacenar información crítica o confidencial de los procesos en las estaciones de trabajo.

b. La Dirección de Tecnología debe establecer una estrategia de backup de información crítica almacenada en los servidores que soporte los requerimientos de recuperación y continuidad de la organización.
c. Es responsabilidad del Oficial de Seguridad de la información y ciberseguridad de la organización la supervisión periódica de los procesos de toma de backup, rotación, custodia y almacenamiento de las cintas de backup.
d. Los medios magnéticos utilizados para realizar las copias de seguridad de la información sensible se deben almacenar en un sitio externo a las instalaciones de la organización. El sitio externo debe cumplir con las condiciones ambientales adecuadas para almacenamiento de medios magnéticos.
e. Trimestralmente, se deben realizar pruebas de restauración de una cinta de backup para verificar el contenido y la usabilidad de la cinta.

5.3.5.1.7 Registro de actividad y supervisión

a. Los sistemas de información que procesan y/o almacenan información crítica y sensible para la operación del negocio e información confidencial deben registrar las actividades de los usuarios en registros de auditoría. Los registros de auditoría deben incluir:

- Identificación de los usuarios
- Fecha y hora de los eventos
- Identificación o dirección IP del computador desde el que se hace la conexión.
- Intentos fallidos de conexión
- Cambios de configuración del sistema
- Uso de utilidades del sistema
- Archivos usados y tipo de interacción
- Cambios a los registros con información confidencial.
- Operaciones privilegiadas

- Intentos de acceso no autorizado
- Cambios o intento de cambios a los parámetros de seguridad de los sistemas de información.

b. Los registros de auditoría deben ser revisados periódicamente por un ente de control
c. El acceso a los registros de auditoría, deben estar restringidos al Oficial de Seguridad de la información y ciberseguridad, Auditoría Interna y administradores de los sistemas de información.
d. Todas las actividades realizadas por los usuarios con privilegios de administración y operación sobre los sistemas de información deben ser registradas en logs de auditoría. Estos logs deben incluir:

    - Identificación del usuario administrador y/u operador
    - Fecha y hora del evento
    - Información del evento

e. Las fallas y los errores de los sistemas de información se deben registrar y analizar para determinar el plan de acción apropiado.
f. Los relojes de los diferentes sistemas de información deben estar sincronizados con la hora legal de Colombia definida por el Instituto Nacional de Metrología.

5.3.5.1.8 Gestión de las vulnerabilidades técnicas

a. La Dirección de Tecnología con el apoyo del Oficial de Seguridad de la información y ciberseguridad de la Organización, debe realizar cada seis meses una prueba de ethical hacking y análisis de vulnerabilidades en los equipos que soportan los aplicativos críticos y misionales.

b. Se debe desarrollar un plan de tratamiento para mitigar los riesgos identificados en las pruebas de ethical hacking

5.3.6 Seguridad en las telecomunicaciones

5.3.6.1 Gestión de la seguridad en las redes:

a. La Dirección de Tecnología debe establecer los acuerdos de nivel de servicios necesarios en los enlaces de comunicaciones para la correcta operación, adicionalmente, debe coordinar con los proveedores externos la implementación de estos niveles de servicio.
b. La Dirección de Tecnología debe coordinar la implementación de los siguientes controles en las conexiones de red son:

    - Los procedimientos de administración y operación de las redes de comunicaciones deben estar debidamente documentados y protegidos contra acceso no autorizado.
    - Los puntos de conexión física a la red cableada que no estén siendo utilizados se deben desconectar
    - Controles mediante filtros de direcciones MAC para las redes inalámbricas.
    - Monitorear la disponibilidad de las redes de comunicaciones

5.3.6.2 Mecanismos de seguridad asociados a servicios de red

5.3.6.2.1 Normas en el uso de internet

a. El jefe inmediato debe aprobar el acceso a internet de sus colaboradores.

b. El acceso a internet NO puede ser utilizado para los siguientes propósitos:
    - Actividades relacionadas a juegos online por internet
    - Ingreso a cualquier material considerado como pornográfico, ofensivo, discriminatorio o ilegal según las normas internas de la Organización y la legislación vigente
    - Descargar música, videos, fotos, fondos de pantalla, programas, juegos etc., los cuales representan un alto riesgo de virus y daños al computador y de legalidad en su uso por derechos de autor.
    - Cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocios particulares.
    - Utilizar los servicios de internet para la transmisión, distribución o almacenamiento de cualquier archivo protegidos por derechos de autor, marcas registradas, secretos comerciales u otros de propiedad intelectual.
    - El acceso no autorizado a cualquier intento de prueba, verificación o rastreo (scan) de vulnerabilidades de un sistema o red.
    - No está permitido el acceso a redes sociales.

5.3.6.2.2 Intercambio de información con partes externas

a. El Oficial de Seguridad de la información y ciberseguridad con el apoyo de la Dirección de Tecnología debe documentar los procedimientos y controles para el intercambio de información utilizando medios digitales. Los controles que se deben tener en cuenta son:

    - El intercambio de información debe ser aprobada por el dueño de la información y/o la Gerencia de la Organización.
    - Se debe proteger la información confidencial contra intercepción, copia, modificación o destrucción.

- Detección de software malicioso que pueda ser transmitido.
- Informar a todos los funcionarios y externos sus responsabilidades con el cumplimiento de las políticas y procedimientos para el intercambio de información.
- Concienciar a los funcionarios y terceros acerca de las precauciones que deben tener cuando exponen información confidencial en conversaciones personales o telefónicas.
- Concienciar a los funcionarios y terceros en que no deben dejar mensajes con información confidencial en ningún tipo de contestador o buzón telefónico.

b. Los funcionarios que requieran enviar y/o recibir información de un tercero, deben establecer un acuerdo de intercambio en el que se deben tener en cuenta:

- El intercambio de información con terceros se debe realizar exclusivamente si existen razones del negocio.
- El intercambio de información clasificada como confidencial con un tercero, debe ser aprobado por el dueño de la información.
- Se deben definir claramente los responsables del envío, recepción y notificación del intercambio de información.
- Se deben definir los acuerdos de retención de dicha información.
- Se deben definir las responsabilidades y responsables de incidentes de seguridad de la información.
- Establecer las responsabilidades de derechos de autor y licenciamiento

5.3.7 Adquisición, desarrollo y mantenimiento de los sistemas de información

5.3.7.1 Seguridad en los procesos de desarrollo, adquisición y soporte

a. La Dirección de Tecnología debe desarrollar e implementar una metodología formal para el desarrollo de software. Esta política debe cumplir con las políticas y normas de seguridad establecidas en la Organización
b. La Dirección de Tecnología de la Organización debe implementar un procedimiento formal y documentado para la solicitud de un nuevo desarrollo o adquisición de software aplicativo.
c. Todo el software desarrollado, adquirido o modificado debe corresponder a una solicitud formal del dueño de la información.
d. Para la adquisición o desarrollo de software, se deben tener en cuenta las siguientes normas:

    - El dueño de la información debe incluir en la solicitud de adquisición tanto los requerimientos funcionales como los requerimientos de seguridad. Los requerimientos de seguridad deben estar acordes con el nivel de clasificación de la información que administra el aplicativo y deben ser aprobados por el oficial de seguridad de la información de la Organización.
    - La solicitud de adquisición y/o desarrollo de software debe ser evaluada a la luz de un caso de negocio, en donde se especifique por parte del solicitante los beneficios operacionales, económicos, comerciales y/o estratégicos que se obtendrán.
    - La aprobación final del desarrollo y/o adquisición de software debe ser otorgada por la gerencia y el director de tecnología, quienes a su vez determinará el nivel de prioridad con la cual se debe realizar el cambio.
    - Debe incluirse dentro de la solicitud de la adquisición y/o desarrollo de software, que es de obligatorio cumplimiento la entrega de los manuales de la aplicación en la versión correspondiente y/o la actualización de la documentación existente.

- Los desarrollos, adquisiciones y mantenimientos de software realizados por personal interno o externo deben cumplir las políticas, normas, procedimientos, estándares de desarrollo de software y seguridad de la información formalmente establecidos en la Organización.

5.3.7.2 Procedimiento de control de cambios de software

a. Todo software nuevo o modificado debe ser probado y aprobado de acuerdo con los procedimientos de control de cambios definidos por la dirección de tecnología.
b. Todas las modificaciones significativas, actualizaciones importantes y nuevos sistemas deben ser aceptados y probados por los dueños de información antes de su instalación en producción. El plan de aceptación del usuario incluirá pruebas de los principales procesos, funciones e interconexión con otros sistemas. La metodología de pruebas se debe documentar en los formatos definidos.
c. Durante la prueba de aceptación, los desarrolladores no pueden modificar el código fuente que se está evaluando. Si se identifican errores, el usuario debe documentarlos. El desarrollador debe hacer las modificaciones necesarias en el ambiente del desarrollo y una vez finalizadas reportar al administrador del sistema para que se realicen nuevamente las pruebas.
d. La Dirección de Tecnología debe conservar todos los formatos de requerimientos de cambio, cronogramas de prueba de cambios y resultados de las pruebas.

5.3.7.3 Revisión técnica de las aplicaciones por cambios en los sistemas operativos

a. Cuando se requiera hacer un cambio de alto impacto al sistema operativo de los servidores que soportan el aplicativo la Organización (cambios de versión o de releáse), antes de realizar el cambio se deben hacer pruebas en ambientes controlados para determinar los efectos que tendrá el cambio en los ambientes de producción. El resultado de las pruebas es satisfactorio, se procede a programar el cambio siguiendo el procedimiento establecido.
b. Después de implementar cambios de alto impacto en los sistemas operativos de los servidores de misión crítica, se debe hacer una revisión de la funcionalidad y seguridad del aplicativo por parte de los dueños de la información.

5.3.8 Seguridad en las relaciones con terceros

a. Todos los contratistas de servicios externos de la Organización deben firmar un acuerdo de confidencialidad de la información a la cual tengan acceso en el desarrollo de las actividades contratadas.
b. El acuerdo de confidencialidad con terceros debe estar vigente durante todo el tiempo de relación comercial o laboral con el contratista de servicios externos.
c. El acuerdo de confidencialidad con los contratistas de servicios externos debe establecer que toda la información a la cual tengan acceso es de propiedad de la Organización, por lo cual la Compañía se reserva el derecho para analizar y monitorear el uso que los contratistas de servicios externos le den a esta información.
d. Cuando exista una necesidad estricta del negocio para la conexión de terceros a la red local de la Organización, el Oficial de Seguridad de la información y ciberseguridad debe realizar un análisis de riesgos con el fin de identificar los controles aplicables desde el punto de vista de seguridad.
e. Todas las conexiones entre la Organización y las entidades externas deben limitar a los equipos y aplicaciones específicas que se deben trabajar. No se debe permitir el acceso ilimitado a las redes y sistemas de información de la Organización a personal de terceros.

f. Una vez el contratista de servicios externos haya culminado sus actividades comerciales con la Organización, debe retornar y/o destruir toda la información confidencial almacenada en sus equipos en el desarrollo de las actividades.

5.3.9 Seguridad en la continuidad del Negocio de la Organización

a. La Organización debe diseñar, implementar, operar, probar, difundir y mantener un plan de continuidad para los procesos críticos del negocio. Los responsables por la documentación, pruebas y seguimiento del BCP serán los dueños de cada proceso.
b. El plan de continuidad del negocio de la Organización debe garantizar la protección de las personas y la restauración oportuna y ordenada de los procesos y servicios en caso de un incidente que afecte la continuidad en las operaciones.
c. Se debe realizar una evaluación formal de riesgo y un análisis de impacto sobre el negocio (BIA - Business Impact Assessment), para determinar los requerimientos de la Organización, identificar eventos que puedan causar interrupciones a los procesos del negocio. Dentro de las amenazas incluir:

- Desastres naturales
- Fuego
- Pérdida de servicios públicos críticos de la infraestructura tales como energía, comunicaciones o agua.
- Enfermedad del personal
- Huelgas o interrupciones laborales.
- Fallos del hardware
- Fallos del software

- Ataques de código malicioso.
- Ciberataques
- Robo de información confidencial
- Desorden civil
- Bloqueos del transporte público
- Vandalismo

d. Las etapas que conforman la metodología del plan de continuidad de la Organización deben ser ejecutadas con la siguiente frecuencia:

- BIA – análisis de impacto al negocio se debe realizar cada 12 meses o cuando se presenten cambios en la estructura del mapa de procesos de la Organización.
- La gestión de riesgos de continuidad se debe monitorear cada 6 meses.
- Se deben realizar 2 pruebas del BCP al año.

e. Todos los funcionarios de la Organización deben conocer el Plan de Continuidad del Negocio y sus responsabilidades dentro de él.

f. La actualización del Plan de Continuidad del Negocio se debe dar si se presentan uno o más de los siguientes casos:

- Adquisición de nuevos equipos
- Actualizaciones en los sistemas operativos
- Actualización o cambio del sistema de información principal
- Ingreso o cambio de Personal
- Cambio en Direcciones o números telefónicos
- Cambio en las Estrategias de negocio
- Cambio de las instalaciones físicas
- Nuevas normas y/o regulaciones internas o externas

- Nuevos contratistas, proveedores de servicio y/o clientes
- Procesos nuevos o eliminados
- Actualización de la matriz de Riesgo (Operacional y financiero)

g. Los procesos o actividades que sean delegadas a terceros deben disponer de planes de continuidad del negocio, por lo tanto, antes de oficializar los contratos con terceros, se debe verificar la existencia de el plan de continuidad y durante la relación contractual se debe verificar por parte del gestor del contrato que los planes son probados y funcionan en las condiciones esperadas.

5.3.10 Cumplimiento de los requisitos legales y contractuales

5.3.10.1 Derechos de propiedad intelectual (DPI)

a. El software utilizado en los PC y/o servidores de la Organización debe estar debidamente licenciado.
b. Los funcionarios de la Organización deben cumplir las leyes y las restricciones de derechos de autor definidos por el fabricante de los aplicativos utilizados.
c. La instalación de software en las estaciones de trabajo y/o servidores de la Organización debe ser aprobado por la dirección de tecnología
d. El software desarrollado por o para la Organización es de propiedad de la organización. El software desarrollado por empleados de la entidad durante su permanencia en la entidad se considera propiedad de la Organización.
e. La Dirección de Tecnología debe realizar revisiones periódicas al software instalado con el fin de identificar software que no cumpla con los derechos de autor y acuerdos de licenciamiento.

f. Está totalmente prohibido realizar copias parciales o totales de libros y/o software que esté protegido por leyes de derechos de autor.

5.3.10.2 Protección de datos y privacidad de la información personal

a. La Organización debe diseñar e implementar los controles necesarios para proteger los datos personales de funcionarios o terceros contra acceso y divulgación no autorizada.

5.3.10.3 Revisiones de la seguridad de la información y ciberseguridad

a. El Oficial de Seguridad de la información y ciberseguridad debe revisar periódicamente el cumplimiento de las políticas, normas y procedimientos de seguridad de la información y ciberseguridad. En caso de identificar incumplimiento de estas, de iniciar el procedimiento de gestión de incidentes de seguridad.
b. Los directores las áreas de la Organización deben reportar al Oficial de Seguridad de la información y ciberseguridad cuando se observe incumplimiento de las políticas y/o normas de seguridad de la información y ciberseguridad.
c. Los directores de las áreas de la Organización deben revisar regularmente los procedimientos de su área para asegurar que se cumplen razonablemente.
d. El Oficial de Seguridad de la información y ciberseguridad debe verificar que los directores de las diferentes áreas gestionen adecuadamente el cumplimiento de las normas y procedimientos de seguridad de la información y ciberseguridad.

6 CONCLUSIONES

En la monografía propuesta se concluye que las organizaciones al no tener un modelo a seguir de políticas de seguridad definidas es muy importante aplicarlas en una de las reglas definidas por el administrador de la seguridad de la información escogido al interior de la organización para evitar robos o fugas de información.

Al analizar los riesgos y vulnerabilidades que puede presentar un servidor de información se da por sentado que estandarizar el uso de mecanismos de seguridad al interior de las organizaciones a partir de un buen modelo de políticas de seguridad preestablecidas según la necesidad de esta ayuda a disminuir el número de incidentes de seguridad que se presentan al interior de ella.

Las estrategias actuales deben ser basadas en la normatividad vigente como lo es la ISO 27001 ya que comprende y encierra los aspectos más importantes de la seguridad de la información, además que nos facilita las herramientas para establecer un buen plan de trabajo en nuestras organizaciones, marcadas con la mejor manera de aplicar seguridad actualmente.

La aplicación del modelo de políticas de seguridad presentado anteriormente es solo el comienzo para realizar una buena administración de los incidentes de seguridad al interior de una organización, el conocer la familia de amenazas existentes tanto físicas como a nivel de software ayuda a construir modelos independientes que ayuden a la seguridad en cada una.

Capacitar a los empleados para que se cumplan las políticas de seguridad que se emplearon en la gestión de riesgos.

Para minimizar los riesgos encontrados en los activos de la organización se recomienda la creación de un departamento especializado en el mantenimiento de los equipos y que a la vez los profesionales encargados del área estén en permanente capacitaciones frente a los avances tecnológicos.

Es importante establecer un plan de seguimiento a las amenazas y riesgos salvaguardados, con la finalidad de que estén en constante revisión y supervisión, para estar a tono con la velocidad de avances tecnológicos con la finalidad de prevenir futuros ataques.

7 RECOMENDACIONES

La implementación de políticas de seguridad de la información no solo es para cumplir con parámetros establecidos en la norma ISO 27001 también para realizar un seguimiento según ciclo PHVA y evaluar el cumplimiento real de los controles, la auditoria es necesaria para revisar que tan eficiente están siendo los controles

También es necesario que la alta gerencia incluya el tema de capacitaciones de manera periódica a todo el personal involucrado en la implementación del sistema de gestión de seguridad de la información.

Las organizaciones deben tener identificadas las necesidades frente a los activos de información que manejan y su impacto según la integridad disponibilidad y confidencialidad de la información y así determinar que salvaguardas se deben implementar para mitigar incidentes de de impacto critico en el negocio.

8 BIBLIOGRAFÍA

AGUIRRE CARDONA, J. D., & ARISTIZÁBAL BETANCOURT, C. (2013). Obtenido de: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf;jsessioni d=75BA0F422DA002AC4D56DA871D477626?sequence=1

ALEMÁN NOVOA, H., & RODRÍGUEZ BARRERA, C. Metodología para el análisis de riesgos en los SGSI. (2015) Obtenido de Publicaciones e Investigación EAN: http://hemeroteca.unad.edu.co/index.php/publicaciones-einvestigacion/article/view/1435/1874

ÁLVAREZ BASALDÚA, Luis Daniel," seguridad en informática auditoría de sistemas". en línea. (18 de marzo de 2017) Disponible en: http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

ÁLVAREZ, M. G., & PÉREZ, G. P. P. Seguridad informática para empresas y particulares (2004). España: McGraw-Hill España. P 20 - 41 Recuperado de: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10498593&tm=1466006497840

ARIAS VALENCIA, M. M. La triangulación metodológica: sus principios, alcances y limitaciones. (abril de 1999). Obtenido de Udea.com: https://www.uv.mx/mie/files/2012/10/Triangulacionmetodologica.pdf

ÁVILA GARCÍA, V. La triangulación, una técnica de investigación. (8 de octubre de 2010). Obtenido de Triangulación: http://triangulacion-tecnicadeinvest.blogspot.com.co/

BENÍTEZ, MOISÉS. Políticas de seguridad informática [en línea]. En: Gestión integral. 2013. no. 1, p. 8. [citado el 16-04-16]. Disponible en: http://www.gestionintegral.com.co/wpcontent/uploads/2013/05/Pol%C3%ADticasde-Seguridad-Inform%C3%A1tica-2013-GI.pdf

C.M., J. Metodologías de Evaluación en Riesgos Informáticos. (23 de marzo de 2014). Obtenido de http://metodosdeevaluacionderiesgos.blogspot.com.co/2014/03/metodologias-deevaluacion-de-riesgos.html

COBIT, CMMI, PMBOK: Como integrar y adoptar los estándares para un buen Gobierno de TI: https://helkyncoello.wordpress.com/2008/12/08/itil-cobit-cmmi-pmbok-como-integrar-y-adoptar-los-estandares-para-un-buen-gobierno-de-ti/

COELLO, H. Información de interés del mundo TI. Obtenido de ITIL, Escrivá, G. G., Romero, S. R. M., & Ramada, D. J. Seguridad informática. (2013). España: Macmillan Iberia, S.A. P 6 - 78 Recuperado de: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=2&docID=10820963&tm=1466006456772

GUERRERO CLAVIJO JAIME, Manual de políticas de Seguridad de la Información (02 mayo 2017) Recuperado de file:///C:/Users/adriana.onate.GRUPOASA/Downloads/VERSION%20FINAL-%20ya%20corregida-%20julio%2018.pdf

HURTADO DE BARRERA, Jacqueline. La investigación proyectiva [en línea]. s.l.: Blogspot.com, 2008. Disponible en: http://investigación holistica.blogspot.com.co/2008/02/la-investigacin-proyectiva.html

ISOTools Excelence (2014) de ISOTools Excellence Recuperado de: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

LÓPEZ NEIRA, A., & RUIZ SPOHR, J. ISO 27000.ES. (2005). Obtenido de El portal de ISO 27001 en español: http://www.iso27000.es/index.htm

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Fortalecimiento de la gestión TI en el estado [en línea]. Bogotá: El autor, s.f. [citado el 30-10-16]. Disponible en: http://www.mintic.gov.co/ gestión/615/w3-propertyvalue-6206.html

MINITIC. (s.f.). MINITIC. Obtenido de MINITIC: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

MINITIC. (s.f.). MINITIC. Obtenido de MINITIC: www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Mintic Colombia. Ley 1273 de 2009, (2009). Recuperado de: http://www.mintic.gov.co/portal/604/w3-article-3705.html

MinTic. Seguridad y privacidad de la información. (29 de 07 de 2016). Obtenido de https://www.mintic.gov.co/gestionti/615/articles5482_Modelo_de_Seguridad_Privacidad.pdf

PEN Y GEULAN The ISO 27001 Directory. (2008). Recuperado http://www.27000.org/iso-27001.htm

SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ, Régimen Legal de Bogotá D.C. (25 de marzo de 2017) Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Universidad EAN. “Metodología para la implementación de un Sistema Integrado de Gestión con las normas iso 9001, iso 20000 e iso 27001. ". En linea. (abril de 2017) disponible en: http://repository.ean.edu.co/bitstream/handle/10882/2779/CortesDiana2012.pdf?sequence=2

VARGAS MICHEL, Manual de políticas de Seguridad de la Información. (04-agosto-2017) Recuperado de http://www.carvajaltys.com/wp-content/uploads/2017/11/Pol%C3%ADticas-de-Seguridad-de-la-Informaci%C3%B3n.pdf

Fecha de Realización:	14/12/2020
Programa:	Especialización en seguridad informática
Línea de Investigación:	Monografía
Título:	PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN LAS ORGANIZACIONES
Autor(es):	Adriana Oñate Arboleda
Palabras Claves:	Sistema de gestión de seguridad de la información, políticas, Riesgos, Activos de Información, Confidencialidad, Integridad, disponibilidad.
Descripción:	Las tecnologías de la información generan ciertos beneficios, mejorando la prestación de servicios y haciendo más fácil el cumplimiento de su misión y objetivos estratégicos, sin embargo, hace que se enfrenten a riesgos que pueden afectar drásticamente la integridad, confidencialidad y/o disponibilidad de la información y los recursos de TI que soportan su procesamiento y transmisión. Para enfrentar este reto y teniendo en cuenta que la información es un activo muy importante

	para la Organización, es necesario implementar estrategias y controles que garanticen altos niveles de seguridad a la información, por medio de un Sistema de Gestión de Seguridad de la Información alineado a la norma internacional NTC / ISO 27001:2013. El Sistema de Gestión de Seguridad de la Información basa su funcionamiento en procesos utilizando el modelo PHVA para identificar, implementar, mantener y mejorar los controles necesarios para identificar y gestionar los riesgos inherentes o potenciales de seguridad de la información y ciberseguridad llevándolos a niveles aceptables de riesgo residual. En las organizaciones se debe hacer énfasis en los siguientes aspectos: • Comprender y entender de los requerimientos de seguridad de la información y ciberseguridad. • Identificar los aspectos legales, comerciales y regulatorios relacionados con la seguridad de la información. • Identificar los activos de información y su clasificación según impacto.

	• Identificar, valorar y gestionar los riesgos inherentes o potenciales de seguridad de la información y ciberseguridad de los procesos que hacen parte del alcance del SGSI. • Incluir en el plan de tratamiento de riesgos, los controles definidos en las normas ISO 27001:2013 e ISO 27032:2012 La falta de políticas de seguridad de la información es un problema que confronta las organizaciones con respecto al uso y protección de los activos de información y los riesgos que se encuentran expuestos por situaciones externas e internas. Las políticas de seguridad indican como operar la seguridad e implementan medidas de protección como: identificación de usuarios, control de acceso físico/lógico, respaldo de información, detección de intrusos y plan de contingencia.
Fuentes bibliográficas destacadas: AGUIRRE CARDONA, J. D., & ARISTIZÁBAL BETANCOURT, C. (2013). Obtenido de: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf;jsessioni d=75BA0F422DA002AC4D56DA871D477626?sequence=1	

ALEMÁN NOVOA, H., & RODRÍGUEZ BARRERA, C. Metodología para el análisis de riesgos en los SGSI. (2015) Obtenido de Publicaciones e Investigación EAN: http://hemeroteca.unad.edu.co/index.php/publicaciones-einvestigacion/article/view/1435/1874

ÁLVAREZ BASALDÚA, Luis Daniel," seguridad en informática auditoría de sistemas". en línea. (18 de marzo de 2017) Disponible en: http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

ÁLVAREZ, M. G., & PÉREZ, G. P. P. Seguridad informática para empresas y particulares (2004). España: McGraw-Hill España. P 20 - 41 Recuperado de: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10498593&tm=1466006497840

ARIAS VALENCIA, M. M. La triangulación metodológica: sus principios, alcances y limitaciones. (abril de 1999). Obtenido de Udea.com: https://www.uv.mx/mie/files/2012/10/Triangulacionmetodologica.pdf

ÁVILA GARCÍA, V. La triangulación, una técnica de investigación. (8 de octubre de 2010). Obtenido de Triangulación: http://triangulacion-tecnicadeinvest.blogspot.com.co/

BENÍTEZ, MOISÉS. Políticas de seguridad informática [en línea]. En: Gestión integral. 2013. no. 1, p. 8. [citado el 16-04-16]. Disponible en: http://www.gestionintegral.com.co/wpcontent/uploads/2013/05/Pol%C3%ADticasde-Seguridad-Inform%C3%A1tica-2013-GI.pdf

C.M., J. Metodologías de Evaluación en Riesgos Informáticos. (23 de marzo de 2014). Obtenido de http://metodosdeevaluacionderiesgos.blogspot.com.co/2014/03/metodologias-deevaluacion-de-riesgos.html

COBIT, CMMI, PMBOK: Como integrar y adoptar los estándares para un buen Gobierno de TI: https://helkyncoello.wordpress.com/2008/12/08/itil-cobit-cmmi-pmbok-como-integrar-y-adoptar-los-estandares-para-un-buen-gobierno-de-ti/

COELLO, H. Información de interés del mundo TI. Obtenido de ITIL, Escrivá, G. G., Romero, S. R. M., & Ramada, D. J. Seguridad informática. (2013). España: Macmillan Iberia, S.A. P 6 - 78 Recuperado de: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=2&docID=10820963&tm=1466006456772

GUERRERO CLAVIJO JAIME, Manual de políticas de Seguridad de la Información (02 mayo 2017) Recuperado de file:///C:/Users/adriana.onate.GRUPOASA/Downloads/VERSION%20FINAL-%20ya%20corregida-%20julio%2018.pdf

HURTADO DE BARRERA, Jacqueline. La investigación proyectiva [en línea]. s.l.: Blogspot.com, 2008. Disponible en: http://investigación holistica.blogspot.com.co/2008/02/la-investigacin-proyectiva.html

ISOTools Excelence (2014) de ISOTools Excellence Recuperado de: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

LÓPEZ NEIRA, A., & RUIZ SPOHR, J. ISO 27000.ES. (2005). Obtenido de El portal de ISO 27001 en español: http://www.iso27000.es/index.htm

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Fortalecimiento de la gestión TI en el estado [en línea]. Bogotá: El autor, s.f. [citado el 30-10-16]. Disponible en: http://www.mintic.gov.co/ gestión/615/w3-propertyvalue-6206.html

MINITIC. (s.f.). MINITIC. Obtenido de MINITIC: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

MINITIC. (s.f.). MINITIC. Obtenido de MINITIC: www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Mintic Colombia. Ley 1273 de 2009, (2009). Recuperado de: http://www.mintic.gov.co/portal/604/w3-article-3705.html

MinTic. Seguridad y privacidad de la información. (29 de 07 de 2016). Obtenido de https://www.mintic.gov.co/gestionti/615/articles5482_Modelo_de_Seguridad_Privacidad.pdf

PEN Y GEULAN The ISO 27001 Directory. (2008). Recuperado http://www.27000.org/iso-27001.htm

SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ, Régimen Legal de Bogotá D.C. (25 de marzo de 2017) Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

<table>
<tr><td colspan="2">Universidad EAN. “Metodología para la implementación de un Sistema Integrado de Gestión con las normas iso 9001, iso 20000 e iso 27001. ". En linea. (abril de 2017) disponible en: http://repository.ean.edu.co/bitstream/handle/10882/2779/CortesDiana2012.pdf?sequence=2

VARGAS MICHEL, Manual de políticas de Seguridad de la Información. (04-agosto-2017) Recuperado de http://www.carvajaltys.com/wp-content/uploads/2017/11/Pol%C3%ADticas-de-Seguridad-de-la-Informaci%C3%B3n.pdf</td></tr>
<tr><td>Contenido del documento:</td><td>Plantear políticas de seguridad de la Información
Objetivos específicos:

1. Clasificar los activos de informaciónsegún el impacto que genera la pérdida de confidencialidad, integridad y disponibilidad.
2. mplementar controles según la declaración de aplicabilidad SOA alineada a la norma ISO 27001:2013
3. Proponer políticas de seguridad de la información.</td></tr>
<tr><td>Conclusiones:</td><td>En la monografía propuesta se concluye que las organizaciones al no tener un modelo a</td></tr>
</table>

	seguir de políticas de seguridad definidas es muy importante aplicarlas en una de las reglas definidas por el administrador de la seguridad de la información escogido al interior de la organización para evitar robos o fugas de información. Al analizar los riesgos y vulnerabilidades que puede presentar un servidor de información se da por sentado que estandarizar el uso de mecanismos de seguridad al interior de las organizaciones a partir de un buen modelo de políticas de seguridad preestablecidas según la necesidad de esta ayuda a disminuir el número de incidentes de seguridad que se presentan al interior de ella. Las estrategias actuales deben ser basadas en la normatividad vigente como lo es la ISO 27001 ya que comprende y encierra los aspectos más importantes de la seguridad de la información, además que nos facilita las herramientas para establecer un buen plan de trabajo en nuestras organizaciones, marcadas con la mejor manera de aplicar seguridad actualmente. La aplicación del modelo de políticas de seguridad presentado anteriormente es solo el

	comienzo para realizar una buena administración de los incidentes de seguridad al interior de una organización, el conocer la familia de amenazas existentes tanto físicas como a nivel de software ayuda a construir modelos independientes que ayuden a la seguridad en cada una. Capacitar a los empleados para que se cumplan las políticas de seguridad que se emplearon en la gestión de riesgos. Para minimizar los riesgos encontrados en los activos de la organización se recomienda la creación de un departamento especializado en el mantenimiento de los equipos y que a la vez los profesionales encargados del área estén en permanente capacitaciones frente a los avances tecnológicos. Es importante establecer un plan de seguimiento a las amenazas y riesgos salvaguardados, con la finalidad de que estén en constante revisión y supervisión, para estar a tono con la velocidad de avances tecnológicos con la finalidad de prevenir futuros ataques